



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,529	12/31/2003	Kevin R. Driscoll	256.197US1	5548

21186 7590 12/28/2006  
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.  
P.O. BOX 2938  
MINNEAPOLIS, MN 55402

EXAMINER
----------

YALEW, FIKREMARIAM A

ART UNIT	PAPER NUMBER
----------	--------------

2136

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/28/2006	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/750,529	<b>Applicant(s)</b> DRISCOLL, KEVIN R.	
	<b>Examiner</b> Fikremariam Yalew	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 01 January 1935.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>05/23/2005</u> . | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-35 have been examined.

#### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 24-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

4. Claims 24,28 and 32 are directed to data authentication method that an operational part of application code has not been modified from its as-delivered form. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. Claims 24,28 and 32 are directed to a computer readable media that includes data signals (See Specification 0054). A signal does not fall within one of the four statutory classes of 101. Claims 25-27,29-31,33-35 rejected on the same rational because they are depend on claims 24,28 and 32.

#### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson, P. K., et al (hereinafter referred as Johnson) (W0 00/18162).
7. As per claim 1,13,24: Johnson discloses a method/apparatus/a machine-readable medium comprising: receiving an ephemeral value from a challenging device (See col 6 lines 17-24 and Figs 2,3); retrieving data whose content is known to the challenging device (col 6 lines 25-33 and Fig 2,3); generating a digital signature of the data based on the ephemeral value; and transmitting the digital signature to the device (Col 6 lines 25-33 and Figs 2,3).
8. As per claim 2,25: Jhonson discloses the method wherein receiving the ephemeral value from the challenging device comprises receiving a randomly generated number from the challenging device (See col 6 lines 1-9).
9. As per claim 3,26: Johnson discloses the method wherein retrieving the data comprises retrieving at least part of application code (See col 7 lines 23-30).
10. As per claim 4,27: Johnson discloses the method wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data based on the ephemeral value (col 6 lines 25-33).
11. As per claim 5,28: Johnson discloses a method comprising: receiving, into a response device, an ephemeral value from a challenge device (See col 6 lines 17-24 and Figs 2,3); retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device (col 6 lines 25-33

Art Unit: 2136

and Fig 2,3); generating a hash across the data using the ephemeral value as a key of the hash (Col 6 lines 25-33 and Figs 2,3); and transmitting at least part of the hash to the challenge device(See Col 6 lines 25-33 and Figs 2 step 212B).

12. As per claim 6,29: Johnson discloses the method further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device (See abstract).

13. As per claim 7,30: Johnson discloses the method wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the response device (col 6 lines 25-33 and Fig 2,3).

14. As per claim 8,31: Johnson discloses the method wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the response device (col 6 lines 25-33 and Fig 2,3).

15. As per claim 9,32: Johnson discloses a method comprising: authenticating data having predictable content and stored in an address space of a remote device, the authenticating comprising: generating a random number (See col 10 lines 20-33); transmitting the random number to a remote device presumably having the data (See col 6 lines 17-24 and Figs 2,3); receiving, from the remote device, a first digital signature that is representative of the data (See Col 6 lines 25-33 and abstract); generating a second digital signature based on the random number(See abstract); and comparing the first digital signature to the second digital signature(See abstract).

16. As per claim 10,33: Johnson discloses the method wherein authenticating the data having predictable content comprises authenticating an application executable (col 7 lines 1-3).

17. As per claim 11,34: Johnson discloses the method wherein authenticating the data having predictable content comprises authenticating at least one security parameter (See col 7 lines 1-3).

18. As per claim 12,35: Johnson discloses the method wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature (See abstract and Fig 3).

19. As per claim 14: Johnson discloses the apparatus wherein the I/O logic is to receive the request for authentication from a challenge device, the I/O logic to transmit the cryptographic hash back to the challenge device (See Figs 2,3).

20. As per claim 15: Johnson discloses the apparatus wherein the storage medium is a nonvolatile memory (See col 10 lines 3-16).

21. As per claim 16: Johnson discloses further comprising a data selection logic to select less than all of the data, wherein the at least part of the data is the less than all of the data (See col 6 lines 17-24 and Figs 2,3).

22. As per claim 17: Johnson discloses the apparatus wherein the data selection logic is to select less than all of the data based on a random number based selection of segments of the data (See col 6 lines 17-24 and Figs 2,3).

23. As per claim 18: Johnson discloses the apparatus wherein the data comprises an application to be executed in the apparatus (col 7 lines 1-3).

24. As per claim 19: Johnson discloses the apparatus wherein the data comprises at least one security parameter of the apparatus (See col 7 lines 1-3).

25. As per claim 20: Johnson discloses a challenge device to authenticate data presumably stored in a response device, the challenge device comprising: a storage medium to store a copy of the data presumed to be stored in the response device (See Fig 1 step 128); a key generation logic to generate an ephemeral value (See Fig 1 step 126 and col 6 lines 1-5); an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication(See Fig 2,3 and abstract); a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature(See Fig 2,3 and abstract); and an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature(See Fig 2,3 and abstract).

26. As per claim 21: Johnson discloses the challenge device wherein the ephemeral value comprises a randomly generated value (See col 6 lines 1-3).

27. As per claim 22: Johnson discloses the challenge device wherein the data comprises application code to be executed by the response device (col 7 lines 1-3).

28. As per claim 23: Johnson discloses the challenge device wherein the data comprises at least one configuration parameter of the remote device (col 7 lines 1-3).

Art Unit: 2136

**Conclusion**

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

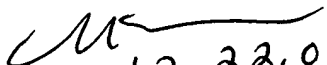
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew  
12/22/06  
FA

Art Unit 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
12,22,06